

The Security Incident Cycle of Ports*

C. Ariel Pinto, Ph.D.
Assistant Professor
Engineering Management and Systems Engineering
College of Engineering
Old Dominion University
Norfolk, Virginia 23529
cpinto@odu.edu

Wayne K. Talley, Ph.D.
Professor of Economics
Executive Director, Maritime Institute
College of Business and Public Administration
Old Dominion University
Norfolk, Virginia 23529
wktalley@odu.edu

Abstract

The security incident cycle of ports consists of four phases: 1) prevention – creates barriers that deny terror plans and events; 2) detection – provides early apprehension; 3) response – pursues an event and mitigates its impact; and 4) recovery – involves the return to normal operations. There have been significant improvements in securing (prevention and detection) ports, i.e., the investigation of ex ante security incidents since the events of September 11, 2001. However, there has been little investigation of ex post port security incidents, i.e., the response and recover once a security incident has occurred. This paper provides an investigation of the security incident cycle of a port by investigating how ports and governments have heretofore addressed prevention and detection of and response and recovery from port security incidents.

*This study was supported by a grant from the Summer Experience Enhancing Collaborative Research Program, Old Dominion University Office of Research.

1. Introduction

The U.S. is the world's largest importer and exporter, accounting for nearly 20 percent of the annual world ocean-borne trade. U.S. ports handle approximately 2 billion tons of cargo annually, expected to double within 15 years (Nagle, 2005), and 7,500 commercial vessels make 51,000 annual calls at 361 U.S. ports. Seven million containers are unloaded annually at U.S. container ports, expected to more than

double in 20 years (Makrinos, 2004).¹ A single U.S. import transaction typically involves 30 different documents and at least 25 parties – making it difficult to accurately track what is coming into the country and the port an attractive and potentially vulnerable target for terrorists (Cooperman, 2004). The rising volume in U.S. world trade has also increased this vulnerability.

The key steps for intercepting and neutralizing a port security threat are delay, detect, respond and mitigate (Emerson and Nadeau, 2003). The delay of an attack relies on buffers such as fences and locked gates to impede approach to a facility. Detection typically utilizes hardware with human interpretation, e.g., cameras and sensors that feed information to security personnel. In response to an attack, personnel intervene between the threat and the threatened facility or immediately act to thwart the attack. Mitigation requires preplanning and trained facility workers to interpret the nature of the breach, decisions (e.g., evacuation) on effective procedures to neutralize the breach's impact and follow-up from law enforcement and emergency response organizations.

Port-security prevention (pre-attack), mitigation and recovery (consequence) programs are required to sustain port security (Harrald et al., 2004). These programs consider the causal chain of events leading to a security incident and the system of systems nature of ports. Ports are critical nodes in the movement of the world's cargo by inter-modal transportation systems.

The cycle that a port experiences in addressing terror events consists of four phases: 1) prevention – creates barriers that deny terror plans and events; 2) detection – provides early apprehension; 3) response – pursues an event and mitigates its impact; and 4) recovery – involves the return to normal operations (Price, 2004). Significant improvements have been made in securing (prevention and detection) U.S. ports, i.e., the investigation of ex ante security incidents since the events of September 11, 2001. However, there has been little or no investigation of ex post port security incidents, i.e., the response and recover once a security incident has occurred. The latter may be attributed to the absence of a major security incident at U.S. ports.

Port security incidents cannot be prevented with certainty. An optimal port-security incident cycle -- prevention, detection, response and recovery -- strategy is one that maximizes the net benefits (i.e., benefits minus costs) of such a strategy, where the benefits are the cost savings to the port from the strategy and the costs are those attributed to the strategy. The efficient allocation of port resources for the

prevention and detection of and response and recovery from security incidents may be deduced from this optimal port-security incident cycle. Such a strategy may result in ports placing greater emphasis on response and recovery from port security incidents than heretofore (Maritime and Port Security Summit, 2004).

This paper provides an investigation of the security incident cycle of a port by investigating how ports and governments have heretofore addressed prevention and detection of and response and recovery from port security incidents. Such an investigation may provide the foundation for developing an optimal port security incident cycle for allocating a port's security resources. Also, it contributes to the port security literature by noting and classifying -- potential port security incidents based upon occurred port accidents and the events and problems that would occur in the response and recovery phases of a port security accident based upon the responses of a port's stakeholders.

Sections 2 and 3 discuss and classify port accidents and potential security incidents, respectively. Approaches adopted by ports for preventing and detecting security incidents are presented in Sections 4 and 5. Response and recovery to a hypothetical port security incident by port security stakeholders at the Port of Hampton Roads, Virginia are presented in Sections 6 and 7, respectively. Resource allocation in a port security incident cycle is discussed in Section 8. Finally, a summary and conclusions are presented.

2. Port Accidents

A maritime transportation (or port) security incident is an intentional "event resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption that affects the maritime transportation system" (Code of Federal Regulations 33, Sub-chapter H, Part 101, p. 105). The U.S. maritime transportation system comprises: 1,000 harbor channels; 25,000 miles of inland, intra-coastal and coastal waterways; and 3,700 marine terminals that handle cargo and passenger movements.

Unlike port security incidents, port accidents are unintentional events. However, both incidents and accidents may have the same outcome, injuries and property damage. Thus, the study of port accidents may provide useful information in the study and prevention of port security incidents, especially in regard to response and recovery.

Port accidents have been classified by type, origin and cause. classifies these accidents by type, origin

and cause.² In an investigation of port accidents in 95 countries, Darbra and Casal (2004) found that releases (or loss of containment) are the most common type of accident (51%), followed by fires (29%) and explosions (17%). The transport of cargo (56.5%) is the most common origin for a port accident, followed by loading/unloading operations (14.9%). The majority (65%) of transport-origin accidents involve ocean-going vessels (movements in and out of port and ship maneuvering within port), followed by pipeline accidents (12%). Other origins include the process plant, storage, waste and warehouse facilities. The most common cause (43.6%) of a port accident is a collision – between ships or between a ship and dry land or between truck and rail vehicles -- followed by mechanical (18.1%), external (17.0%) and human (15.9%) causes. Common external events that cause port accidents are high winds and fires.

Ronza et al (2003) found that 40% of port accidents occur at sea (approach and manoeuver), 21% on land (storage, process and transport) and the remaining 39% occur at a sea-land interface (loading/unloading and maintenance). The most common types of substances involved in port accidents are crude oil and other oil products. Port accidents that involve the handling and storage of hazardous cargo originate, for example, from hardware failures of ship and loading/unloading equipment and external events such as bad weather (Christou, 1999). For specific examples of the cause of port accidents and their mitigation, see the Appendix.

3. Potential Port Security Incidents

Major U.S. port security fears, for example, include: chemical or nuclear weapons smuggled inside containers that enter U.S. ports; an underwater mine sinking a ship and blocking the channel; and a large ship being pirated and used to crash into a bridge, historic landmark or shore-side tanks holding fuel or hazardous materials. Since there has not been a recorded major security incident at a U.S. port, security incident data from foreign ports and/or U.S. and foreign port accident data may be used to predict potential U.S. port security incidents. These data are the basis for the discussion of the four types of potential port security incidents below – waterside, landside, employee and information.

3.1 Waterside Incidents

Ships in ports are vulnerable to potential terrorist attacks. Specifically, ships in port may be berthed at a pier, at anchorage in the harbor or moving at slow speeds through the harbor's waterway, making them

easy to be intercepted by terrorists on a fast moving boat. Also, commercial ships are generally have small crews that are unarmed, making them vulnerable for terrorist attacks.

A hypothetical waterside port security incident is as follows: A tanker ship transporting heating oil departs the Port of New York/New Jersey. Terrorists with scuba-diving equipment enter the water. The weather is foggy, allowing them to breach port security and reach the departing ship. With the ship moving at a slow speed, the terrorists are able to incapacitate the ship's propeller. The terrorists capture the ship and ascend to its top most floors. The terrorists set the tanker on fire and evacuate. Subsequently, the ship explodes, resulting in injuries and deaths to those on board. The ship sinks in the harbor, blocking its channel.

3.2 Landside Incidents

Ports have large landside perimeters to secure, giving terrorists many potential landside points of entry. Since many ports are located in urban areas, terrorists have many places to hide (Medalia, 2004). The truck is a primary means for transporting cargo to and from ports. The large number of trucks at major container ports increases the probability of terrorists using the truck in a terrorist attack -- transporting themselves and weapons into the port (CRS, 2004).

A hypothetical landside port security incident is as follows: A truck is driven by a terrorist, transporting a container. The container has been intentionally overloaded (i.e., exceeding its designed weight capacity) making its movement by truck unstable. After entering the gate of a port, the terrorist intentionally overturns the truck, striking stacked containers, damaging yard equipment and injuring port workers -- thereby disrupting the port's operation. Terrorists may also use the truck for: smuggling arms and weapons of mass destruction in containers, blocking port landside entrances and access roads and as a collision weapon with a bridge or tunnel to limit access to and from a port.

3.3 Employee Incidents

Container ports have numerous types of equipment for handling containers -- to and from berthed ships and their movements within storage areas. Terrorist employees can use the equipment to damage containers and other equipment in order to disrupt port operations.

A hypothetical employee port security incident is as follows: A port employee (turned terrorist) seeks to disrupt the operations of a port. He intentionally creates an accident at the port's entrance gate (from

within the port) by running a container straddle carrier into a truck that has just entered the gate. Port police and emergency personnel are called to the scene, thereby diverting gate security officials. The diversion allows other terrorists to enter the port through the gate and subsequently disrupt the operations of the port. The terrorists could also have entered the port under false identifications.

3.4 Information Incidents

Aside from waterside, landside and employee sources of security vulnerabilities, computer information systems of the port are also vulnerable. The electronic transfer of information – both within (local area networks) and outside (wide area network) of the port -- makes these systems especially vulnerable. Electronically transferred information, for example, may include that from ship manifests, schedules of ship and truck arrivals, and descriptions of cargo.

4. Security Incident Prevention

Port security can be improved by concentrating on reducing vulnerabilities, thus diminishing the potential of threats. A terrorist attack can be engineered by the application of criminal intent. “The most prevalent threat to port security in the Western Hemisphere remains drug smuggling, followed by cargo threat, stowaways and alien smuggling, and sea robbery in the port or harbor” (U.S. Maritime Administration, 2002, p. 7). There is a potential risk of terrorists adopting pirate tactics or allying with criminal enterprises (Carafano and Kochems, 2005). U.S. flagged vessels and those flagged by countries that are perceived to be U.S. allies in the war against terrorism are becoming preferred piracy targets, thus increasing security requirements for these vessels and U.S. port facilities (Shelley, 2003). U.S. ports remain vulnerable to the kind of speedboat attack that crippled the USS Cole and killed 17 sailors in Yemen in October 2000 (Fields, 2004).

Since September 11, 2001, U.S. and international regulations have created barriers to deny terrorist plans and events. The U.S. Transportation Security Administration (TSA) was established by the U.S. Congress on November 19, 2001 with the enactment of the Aviation and Transportation Security Act. Although TSA’s primary emphasis in its early existence was on aviation security, its mission today is to ensure the security of the transportation of people and goods on all modes of the U.S. transportation system. Improving access control to ports is an important component of port security. Port access-control measures include alarm systems, employee background checks, security patrols, perimeter fencing,

terminal lighting, a closed circuit television system and port access/egress controls on trucks and rail cars (i.e., vehicle checks). The TSA, however, missed its initial August 2004 target date for issuing maritime worker identification cards. Reasons are found in a GAO report (General Accounting Office, 2004). The United Nations' International Maritime Organization (IMO), spurred by the U.S., has established new international requirements to strengthen maritime security. Specifically, the International Ship and Port Security (ISPS) Code was ratified by the IMO in 2002. The Code takes a risk management approach to the security of ships and ports -- monitoring and controlling access, monitoring the activities of people and cargo and ensuring the availability of security communications. Ports are required to have security plans, officers and equipment. Marine terminals which serve seagoing vessels of 500 gross tonnage and upwards on international voyages must comply with the ISPS Code by July 1, 2004.

The U.S. Maritime Transportation Security Act (MTSA) signed into law on November 25, 2002 is designed to protect the nation's ports and waterways from terrorist attacks. The MTSA is based upon a risk-based methodology, focusing on the higher security-risk sectors of the maritime industry. The MTSA is to prevent security incidents in the maritime supply chain, i.e., in the movement of maritime cargo from shipper to consignee with the emphasis on the port link of the chain. The MTSA has incorporated the international requirements contained within the ISPS Code and imposed additional security requirements on certain U.S. flagged vessels and off-shore petroleum and commercial port facilities.

Ports are vulnerable to both physical and cyber attacks, e.g., computer viruses and worms (Brandl, 2003). Following the implementation of the ISPS Code and security measures contained in the MTSA, there has been an increase in law enforcement at U.S. ports, e.g., more canine teams and ID checks (Trunick, 2004). Also, smart boxes and security seals have been recommended for preventing container security incidents.

The implementations of the ISPS code and the MTSA have turned the facilities of U.S. ports into high security prisons (Chopra, 2005). Floating barriers at ports provide physical protection and add a layer of defense by providing the ability to stop attacking vessels as well as increasing the security-breach response time for authorities (Pruitt, 2004). Port security plans include access control, responses to security threats and drills to train staff (Staff, Marine Log, 2004b).

The U.S. Coast Guard has moved aggressively to provide maritime security – e.g., the creation of the

High Interest Vessel Boarding Program, the deployment of Coast Guard personnel as “Sea Marshalls” aboard certain ships entering and leaving ports, and the establishment of port security zones around ships and high-risk port facilities. The Coast Guard has adopted the conventional approach to securing fixed facilities, i.e., installing rings of protection or successive hurdles that must be breached before vulnerable assets are reached (Emerson and Nadeau, 2003).

The layered security defense for U.S. ports consists of four zones: foreign port, offshore, coastal and dockside zones (Emerson and Nadeau, 2003). The foreign port zone (layer 1) is the far-out-to-sea-as-possible security defense for U.S. ports. For a vessel arriving at a U.S. port from a foreign port that has ineffective security measures, the Coast Guard may deny entry or prescribe conditions for entry. The offshore zone (layer 2) includes U.S. waters inside the 200 mile exclusive economic zone but beyond the 12 mile territorial sea. In this zone, ships bound for U.S. ports are now required to provide Advanced Notice of Arrival of at least 96 hours prior to entering a U.S. port. The coastal zone (layer 3) includes U.S. waters that extend inward from the 12 mile territorial sea to the docks and piers of a U.S. port. Today certain high-interest vessels are escorted into port with armed Coast Guard members on board.³ The Sea Marshalls provide security to the pilot and crew during transit, diminishing the potential for hijacking. Under the authority of the U.S. Ports and Waterways Safety Act, the Coast Guard may establish security sub-zones within the coastal zone to safeguard waterways, ports, vessels and waterfront facilities from destruction, sabotage or other subversive acts. To restrict vessels from nearing a particular facility, another vessel or a specified geographic area, 115 security zones have been implemented at U.S. ports since September 11, 2001. The dockside zone (layer 4), i.e., the port, is the focus of this paper.

On March 1, 2003 the U.S. Department of Homeland Security (DHS) was established. The DHS has federal responsibility for strategies, standards and funding for the security of ports and other transportation infrastructures. The U.S. Coast Guard was removed from the Department of Transportation and placed under the authority of the DHS. The Maritime Security Level (MARSEC) system was established by the Coast Guard to indicate the severity of a security threat: 1) level one -- a threat is possible, but not likely; 2) level two -- terrorists are likely active in an area; and 3) level three -- a threat is imminent to a given target.

The U.S. Bureau of Customs and Border Protection (CBP), also a DHS unit, has established

voluntary international programs designed to provide point-of-origin to final destination visibility and control over containerized freight movements. Key voluntary programs include: the Container Security Initiative (CSI), in which CBP works with foreign ports to identify potentially dangerous shipments before they arrive in the U.S., and the Customs-Trade Partnership Against Terrorism (C-TPAT), through which CBP provides streamlined clearance of cargo to shippers that establish appropriate security procedures (Banomyong, 2005). C-TPAT membership was initially limited to shippers and manufacturers but now includes other private businesses along the supply chain such as carriers, brokers, forwarders, terminal operators and ports (Bichou, 2004). By the end of 2004, C-TPAT members included: 9,083 U.S. importers, 2,208 carriers, 1,412 brokers, 393 foreign manufacturers and vendors and a small number of port authorities and marine terminal operators (Keane, 2005).

A factor contributing to the difficulty of protecting ports is the lack of coordination among public and private security organizations that are responsible for port security. The MTSA designated the U.S. Coast Guard's Captain of the Port as the Federal Maritime Security Coordinator with oversight authority for maritime/port security (including jurisdiction of maritime/port land facilities). In addition to the Coast Guard, there are also numerous law enforcement and security organizations involved in port security. If a port security threat exists, one agency (likely the Coast Guard) is expected to take the lead in assigning duties and establishing responsibilities of security personnel.

In 2004 a number of marine terminal operators, vessel operators, port associations, shippers and other port stakeholders involved in the importation of ocean containers to the U.S. formed the Coalition for Secure Ports to lobby for enhanced maritime security. The Coalition's goals to strengthen port security include: 1) requiring enhanced cargo information, e.g., knowing the contents of each cargo container before it enters the U.S.; 2) monitoring the location and security of containers in transit; and 3) implementing a Transportation Worker Identification Credential (TWIC) to ensure the identity and verification of those who have access to cargo.⁴

5. Security Incident Detection

In addition to prevention, ports will also undertake detection procedures -- inspection, tracking and monitoring -- as part of the security cycle in addressing terrorist events. The DHS has recommended

improvements in the inspection of ocean containers, e.g., in inspection equipment and search procedures for nuclear material to prevent terrorists from sneaking weapons of mass destruction into U.S. ports (Ervin, 2004).⁵

Many U.S. ports inspect containers using large radiation detectors costing \$1-2 million. While most ship-to-berth cranes can unload containers at a rate of more than 30 per hour, radiation screening of all containers will limit the process to 20 containers per hour, thus decreasing port productivity. Currently, U.S. ports have the capacity to screen only 2-4 percent of container traffic. By December 2005 the ports of Los Angeles and Long Beach will have ninety Radiation Portal Monitors (RPMs) in operation that can screen all exiting container traffic and vehicles for radiation. Specifically, the RPMs can detect various types of radiation emanating from nuclear devices, dirty bombs, natural sources, special nuclear materials and isotopes commonly used in medicine and industry. The Port of Baltimore has recently installed a \$6 million X-ray machine that can scan a 40 foot container in just 30 seconds.⁶

Tracking containers before they reach U.S. soil (Durstensfeld et al, 2003) may be an effective security detection strategy. The U.S. Coast Guard and Maritime Transportation Act of 2004 extends the MTSA by instructing the Coast Guard to build a vessel tracking system that is consistent with various international treaties. For example, the Coast Guard is working with the IMO to develop an international long-range tracking requirement to enhance vessel visibility for flag, port and coastal states. The U.S. Intelligence Reform and Prevention Act of 2004 authorizes the DHS to prepare a National Transportation Security Strategy. In 2005 the National Maritime Security Advisory Committee held its inaugural meeting. The Committee of 20 industry experts provides guidance on trade and cargo security issues to DHS and CBP. Developing a contingency plan for how to keep commerce flowing is a top priority.

Proposals for tracking containers include radio frequency identification (RFID) tags and electronic seals to detect tampering (Fortner, 2002). However, RFID seals can be reset after unauthorized openings and container doors can be removed and replaced without breaking the seal. A higher level of protection comes from monitoring the contents of the container with radiological, chemical and atmospheric sensors with global positioning capabilities. A wide variety of integrated, disparate sensors are needed to generate a high level of awareness in and around the port, while facilitating, rather than hampering, the flow of cargo (McDonald and O'Sullivan, 2004). The biggest challenge is not the technology (which now exists)

but who will pay for the sensors.

The international transportation of cargo has security holes. One such hole is the lack of real-time supply chain visibility that is all encompassing. As new technologies for port security are developed and government regulations enacted, the amount of data collected for specific movements are growing exponentially. Properly monitored, the data can be used to predict, detect and prevent acts of terror (Cooperman, 2004). A GAO report has recommended the use of a geographic information system (GIS) for computer mapping of information that could be used to respond to threats or attacks. Also, the inspection of empty containers (most overlooked of potential security risks) should be intensified.

The Coast Guard has been criticized for not using the best practices of information technology (Beadle, 2004). The Coast Guard is considering attaching transmitters to buoys of the National Oceanic and Atmospheric Administration (NOAA) to capture cargo and crew information from ships hundreds of miles before they reach port. NOAA uses the buoys to collect data on winds, temperatures and waves. Under the current system the Coast Guard can only gather ship data when the ship is within 25 miles of a port (Staff, 2004a).

6. Security Incident Response

The ISPS Code and the MTSA require that U.S. ports revise their security plans to include deterrence actions for a terrorist attack as well as response actions to reduce the impact of a terrorist attack. The MTSA requires the establishment of committees at U.S. ports to coordinate the security activities of public and private port stakeholders. A particular concern is the coordination of security response and recovery actions by the stakeholders.

The MTSA requires a National Maritime Transportation Security Plan “...for efficient, coordinated and effective action to deter and minimize damage from a transportation security incident...” The Homeland Security Presidential Directive 13 (HSPD-13) of December 2004 states that “expediting recovery and response from attacks within the maritime domain” is one of six core elements of U.S. policy for enhancing the security of this domain. If a major security incident occurs at a port, the likely initial response is to shutdown the port. If the port is shutdown for a significant length of time, the economic loss to the port, e.g., the opportunity cost of cargo revenue foregone, may be greater than the

damage cost from the security incident itself. DHS' "Interim National Preparedness Goal" of March 31, 2005 is "to engage Federal, State, local and Tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to and recover from major events in order to minimize the impact on lives, property and the economy."

Does one port stakeholder have the sole authority to make response and recovery decisions once a port security incident has occurred? Are there several primary port stakeholders for whom their authority depend upon the incident's location or the type of incident? What are the responsibilities of each port stakeholder in responding to a major port security incident?

The above questions were addressed at a recent meeting, "The Roundtable on Continuity of Operations in the Port of Hampton Roads," held on August 2, 2005 in Norfolk, Virginia. Representatives of many of the port's major stakeholders were in attendance:

1. Virginia Port Authority (VPA)
2. Virginia International Terminals (VIT), which operates VPA's marine terminals
3. National Oceanic and Atmospheric Administration (NOAA)
4. Federal Bureau of Investigation (FBI)
5. U.S. Maritime Administration (MARAD)
6. Lambert's Point Docks (a marine terminal owned and operated by Norfolk and Southern railroad)
7. Virginia Marine Police
8. VPA Maritime Incident Response Team
9. Military Surface Deployment and Distribution Command Transportation Engineering Agency, U.S. Army
10. U.S. Coast Guard
11. U.S. Bureau of Customs and Border Protection (CBP)
12. U.S. Army Corps of Engineers
13. Security and Emergency Management, Virginia Department of Transportation
14. Operations and Public Safety, Mid-Atlantic Region, U.S. Navy
15. APM Terminals

The attendees at the roundtable meeting were asked their security response and recovery

actions to the following hypothetical security incident in the Port of Hampton Roads:

A liquefied petroleum gas (LPG) tanker vessel moving slowly through the port's harbor is approached by a small speeding boat with terrorists. The terrorists attach a bomb along the side of the vessel, which subsequently explodes, resulting in a gaping hole about 40 feet long in the vessel's side and the loss of propulsion and electrical power. Several crew members are dead and injured; some are in the water. The LPG vessel drifts toward VPA's Norfolk International Terminals (NIT), VPA's largest marine container terminal. The vessel incurs a second explosion damaging it further as well as damaging a nearby container ship berthed at NIT -- several containers are blown off the berthed ship; some are floating, others are sinking. Several dockworkers that were working the container ship at the time of the blast are either killed or badly injured. The LPG vessel subsequently sinks, blocking the harbor channel -- which is used by commercial as well as U.S. Navy vessels. The Navy's marine terminal is near NIT.

The first responder to the security incident is the Coast Guard. Specifically, the Coast Guard's Captain of the Port who is responsible for the security of the port notifies its sector command and headquarters and the FBI of the security incident. Details of the security incident are reported. The Coast Guard implements security level MARSEC III in the Port of Hampton Roads. The Coast Guard also ascertains the severity of the incident and whether secondary incident impacts (e.g., explosions) and further attacks are expected. It also seeks to mitigate any further attacks by requesting the assistance of the Virginia Marine Police in establishing and policing waterway security zones. The Coast Guard also asks the VPA Maritime Incident Response Team for assistance in eliminating harbor fires and rescuing injured people from the water. This team, in turn, asks the local fire department for assistance.

The VPA shut downs NIT (no inbound and outbound cargo movements) and evacuates personnel. Inbound cargo (via ship, barge, truck and rail) at VPA's other two marine terminals in Portsmouth and Newport News are stopped. VIT seeks to keep the land outbound cargo at these two terminals moving as normally as possible. However, the shutdown and evacuation of NIT precipitates the shutdown of these terminals as well. The sudden shutdown of terminals creates severe congestion at terminal gates and on adjacent roads -- from trucks in route and the

evacuation of terminal workers -- restricting the arrival of emergency vehicles. The VPA requests the assistance of the local police in addressing the road congestion problem.

The FBI's initial response to the incident is to support the Coast Guard in the collection of intelligence with respect to further attacks and the severity of the incident. It also assists the Coast Guard in mitigating further attacks. The U.S. Navy secures its vessels and other assets, i.e., taking care of itself. The CBP has little response except for accounting for personnel and checking suspicious cargo. The two private marine terminals, Lambert's Point Docks and APM Terminals, follow the lead of VPA and are shutdown. The Director of Security and Emergency Management, Virginia Department of Transportation notifies pertinent Virginia state agencies and the Governor's office of the occurrence of the security incident. The Director also requests authorization from the Governor's office for additional state police as well as for troops from the state's National Guard to be sent (if needed) to the Hampton Roads area.

7. Security Incident Recovery

Once the Coast Guard's Captain of the Port announces that the port is secure from terrorist attacks and secondary security incident impacts (e.g., explosions and fires), the security incident recovery phase begins. For the hypothetical security incident in Section 6, the recovery phase begins when marine terminals that were shutdown as a result of the terrorist attack are now open (even on a limited basis). The recovery phase ends when the terminals have resumed normal operations.

In the early stages of the recovery phase (for the above hypothetical incident), import cargo that was stored at marine terminals prior to the security incident is allowed to leave by truck and rail (subject to FBI approval). The FBI gathers evidence at the crime scene, i.e., from the sunken LPG vessel and sunken and floating containers, and interviews eyewitnesses of the incident. The FBI requests that the crime scene not be disturbed and the channel not be reopened. However, because economic losses are incurred by the port and its users -- e.g., VPA, VIT, the private marine terminals, shippers, truckers, railroads and shipping lines -- when the channel is closed, the FBI is under pressure to finish its investigation of the crime scene as quickly as

possible so that the sunken ship can be removed from the channel for its reopening. Since the Hampton Roads area in general will experience economic losses, the FBI is also under pressure from the Governor's office for the reopening of the channel.

Once the FBI has given permission for the sunken ship and other obstructions to be removed from the channel, NOAA is asked to survey the harbor waterways for obstructions. The sunken ship's owner and the owners of sunken and floating containers are responsible for their removal from the channel. If the channel's depth and turn-basin area have been altered, the Army Corps of Engineers will dredge the channel to specifications that existed prior to the security incident. The Coast Guard will decide whether the MARSEC level should be reduced and if so, at what level. The channel is officially opened when so designated by the Captain of the Port.

The time incurred between the re-opening of a marine terminal and its return to normal operations can be investigated using a throughput simulation model of the terminal. Such models in the past have generally been used to investigate inefficiencies in marine terminal operations, but also can be used to analyze security disruptions. Throughput simulation models of port operations include those by: Leathrum et al. (2004) who simulate the operations of a military port; Luo and Grigalunas (2003) who use a spatial-economic simulation approach to modeling a port; and Demirci (2003) who simulate port investments. However, none of these models clearly address the economics of recoverability or the time to recovery from a port security incident. Port simulation models that address the latter may be also be used to predict the total loss in throughput from a security incident until a terminal's normal operations are restored.

8. Resource Allocation in a Port Security Incident Cycle

How much of a given security resource should a port (or marine terminal) allocate to a particular phase of the security incident cycle? In theory, this allocation may be determined by a port maximizing security for the i th security incident phase (prevention, deterrence, response or recovery) subject to a cost constraint for the i th security incident phase, i.e.,

$$\text{maximize } S_i = f(R_{1i}, R_{2i}, \dots, R_{ji}, \dots, R_{ni})$$

subject to $C_i = C_1R_{1i} + C_2R_{2i} + \dots + C_jR_{ji} + \dots + C_nR_{ni}$

where, S_i = security for the i th security incident phase.

R_{ji} = amount of the j th security resource allocated to the i th security incident phase.

C_i = resource cost of the i th security incident phase.

C_j = unit cost of the j th resource.

The S_i security function is an economic production function that relates the maximum security obtainable for the i th security incident phase in the utilization of “ n ” resources. The choice variables in the optimization are the R_{ji} resource variables. The values of these variables that satisfy the optimization are the amounts of the “ n ” resources to be allocated in the provision of security for the i th security incident phase -- i.e., the amounts of resources utilized that will maximize the port’s security for the i th incident phase for a given cost constraint for that phase.

Alternatively, the question may not be whether more security is needed but how much of a given resource is to spent for added security. That is to say, a risk-based return-on-investment (RROI) approach may be used to determine if enough security resources are being spent in light of the reduction in security risk afforded by such resources (e.g., additional perimeter cameras, tighter ID and document authentication, higher fences, etc.).

Arora et al. (2004) have described a framework that integrates risk profile with actual damages and implementation costs of security resources to determine costs and benefits of security solutions. In essence, this framework suggests using the following RROI equation:

$$RROI_k = Ra_k - Oc_k / Oc_k$$

Where ,

$RROI_k$ = return-on-investment of set k of security resources.

Rr_k = residual risk of implementing set k of security resources.

Ra_k = risk avoided by implementing set k of security resources.

Ock = total operating cost of a set k of security resources.

RROI is measured as the ratio between the net benefit in implementing a set of security resources and the cost of implementation. Unlike the conventional notion of ROI that measures

how effectively resources are used to generate profit, RROI measures how effectively resources are used to *avoid or reduce risk*. Specifically, a positive RROI means that the degree of risk avoided is greater than the implementation cost, and a greater RROI means more risk is avoided per dollar spent in implementation. However, positive RROI does not change the fact that security activities are primarily cost centers. It is important to note that RROI should be used to guide overall investment in security such that investments should be made until the RROI falls to the minimum acceptable rate.

9. Summary and Conclusions

This paper has provided an investigation of the security incident cycle of a port by investigating how ports and governments have heretofore addressed prevention and detection (*ex ante*) of and response and recovery (*ex post*) from port security incidents. A port security incident is an intentional event, whereas a port accident is an unintentional event. Both port security incidents and accidents may have the same outcome, injuries and property damage. Since there has not been a recorded major security incident at a U.S. port, the study of port accidents may provide useful information in the prevention of potential U.S. port security incidents. Potential port security incidents may be classified as waterside, landside, employee and information accidents.

The security incident cycle of a port consists of the prevention, detection, response and recovery phases. There have been significant improvements in the prevention and detection phases, but little investigation of the response and recovery phases (*i.e.*, once an incident has occurred) of a port's security incident cycle. Prevention strategies, for example, include the: (1) establishment of the U.S. Transportation Security Administration (TSA) to secure the transportation of people and goods by all U.S. modes (*e.g.*, with alarm systems, employee background checks and security patrols); (2) passage of the International Ship and Port Security (ISPS) Code (a risk management approach to the security of ships and ports); (3) Coast Guard's layered security defense for U.S. ports; and (4) establishment of voluntary port security programs by the U.S. Bureau of Customs and Border Protection (CBP) such as the Container

Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) programs. Detection strategies include: (1) port radiation detectors and (2) the tracking of containers, e.g., radio frequency identification (RFID) tags.

The Homeland Security Presidential Directive 13 (HSPD-13) of December 2004 states that “expediting recovery and response from attacks within the maritime domain” is one of six core elements of U.S. policy for enhancing the security of this domain. A particular concern is the coordination of security response and recovery actions by the port’s stakeholders. This coordination was investigated at a meeting of the stakeholders at the Port of Hampton Roads (Norfolk, Virginia) in August 2005 for a hypothetical major port security incident involving a LPG tanker vessel: The Coast Guard is the first responder; the Coast Guard’s Captain of the Port notifies its sector command and the FBI. The Coast Guard ascertains the severity of the incident and whether secondary impacts are expected. The Virginia Port Authority shuts down the port and its Maritime Incident Response Team assists in eliminating harbor fires. The state’s Director of Security and Emergency Management notifies pertinent state agencies and the Governor. In the early stages of the recovery phase, the FBI gathers evidence at the crime scene and requests that the scene not be disturbed (including closure of the harbor’s channel). However, because economic losses are incurred by the port and its users, the FBI will be under pressure to finish its investigation as soon as possible. The channel is officially opened when so designated by the Captain of the Port. The recovery phase ends when the port has resumed normal operations.

Endnotes

1. For a discussion of ocean container transportation, see Chadwin, Pope and Talley (1990) and Talley (2000).

2. The port accidents are found in the Major Hazard Incident Data Service (MHIDAS), developed and managed by the Safety and Reliability Directorate as a representative of the Major Hazard Assessment Unit of the U.K. Health and Safety Executive. This database was created in 1980 and is updated periodically; it also includes accidents that occurred prior to 1980.

3. On March 1, 2003 the Coast Guard became a component of the newly formed Department of Homeland Security (DHS).

4. A seamen’s rights group has requested that the DHS permit internationally-acceptable merchant mariner identification cards as a substitute for a D-1 visa, so more mariners can take shore leave at U.S. ports.

5. In Israel's Port of Ashdod, Palestinian bombers were smuggled into the port in a shipping container. An inspection of the container by security guards at the Gaza border failed to detect the false panel concealing the bombers.

6. The effectiveness of detectors in detecting biological, chemical, nuclear and explosive terrorist devices may be investigated via mock threat training exercises.

References

- Arora, A. Hall, D., Pinto, A., Ramsey, D. and Telang, R. (2004) Measuring the Risk-Based Value of IT Security Solutions, *IEEE IT Professional*, 6, pp. 35-42.
- Banomyong, R. (2005) The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management, *Maritime Policy and Management*, 32, pp. 3-13.
- Beadle, A. (2004) Coast Guard Faulted on Port Security Review, *Journal of Commerce*, October 1, p. 1.
- Bichou, K. (2004) The ISPS Code and the Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management, *Maritime Economics and Logistics*, 6, pp. 322-348.
- Carafano, J. J. and Kochems, A. (2005) *Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism*, Washington, D. C.: The Heritage Foundation.
- Chadwin, M., Pope, J. and Talley, W. K. (1990) *Ocean Container Transportation: An Operational Perspective*, New York: Taylor and Francis.
- Chopra, A. (2005) ISPS Code: Is the World Safer Today? *Marine Log*, 110, pp. 23-27.
- Christou, M. D. (1999) Analysis and Control of Major Accidents from the Intermediate Temporary Storage of Dangerous Substances in Marshalling Yards and Port Areas, *Journal of Loss Prevention in the Process Industries*, 12, pp. 109-119.
- Clovis, M. (1998) Design of Anchor Pile for Ship Mooring Facilities, *Ports - Proceedings*, 2, pp. 890-896.
- Code of Federal Regulations* 33, Sub-chapter H, Part 101, p. 105.
- Cooperman, S. (2004) Tracking Cargo, *Security*, 41, pp. 20-22.
- Darbra, Rose-Mari and Casal, Joaquim (2004) Historical Analysis of Accidents in Seaports, *Safety Science*, 42, pp. 85-98.
- Demirci, E. (2003) Simulation Modelling and Analysis of a Port Investment, *Simulation*, 79, pp. 94-105.
- Durstenfeld, B., Fuhr, P., Haag, W., Hsi, P. and Ng, J. (2003) Cargo Container Security, *Occupational Health and Safety*, 72, p. 28.
- Dutton, K. (1998) Forecasting Improved Safety and Cost-Savings, *Dock and Harbour Authority*, 79, p. 88.
- Eastaugh, P. (1999) Tracking Technology Brings Benefits to Harbour Operators, *Dredging and Port Construction*, 26, p. 18.
- Emerson, S. D. and Nadeau, J. (2003) A Coastal Perspective on Security, *Journal of Hazardous Materials*, 104, pp. 1-13.

- Ervin, C. K. (2004) Report Cites Port Security Gaps, *Journal of Commerce*, October 14, p. 1.
- Fields, G. (2004) World Customs Body Urges Strict, Uniform Security, *Wall Street Journal*, July 2, p. A4.
- Flory, J. F., Banfield, S. P. and Ractliffe, A. (1998) Computer Mooring Load Analysis to Improve Port Operations and Safety, *Ports – Proceedings*, 2, pp. 840-849.
- Fortner, B. (2002) Electronic Seals Track Containers to Improve Port Security, *Civil Engineering*, 72, p. 37.
- General Accounting Office (2004) *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, Washington, D. C.: U.S. Government Printing Office
- Ghys, R. (1988) Vital Link in the Chain, *Hazardous Cargo Bulletin*, 9, pp. 51 and 53.
- Harrald, J.R., Stephens, H. W. and vanDorp, J. R. (2004) A Framework for Sustainable Port Security, *Journal of Homeland Security and Emergency Management*, 1, p. 3.
- Harrington, L. (1994) Just Say Yes to Workplace Safety, *Transportation and Distribution*, 35, pp. 32-34.
- Keane, A. G. (2005) Applauding C-TPAT's Reach, *Traffic World*, April 25, pp. 9-10.
- Kim, J. W. (1998) Harbor Tranquillity Analysis for Cheonha Harbor, Korea, *Proceedings of the International Offshore and Polar Engineering Conference*, 3, pp. 643-649.
- Knott, M., Wood, D. and Bonyun, D. (1985) Risk Analysis for Ship-Bridge Collisions, *Coastal Zone: Proceedings of the Symposium on Coastal and Ocean Management*, 2, pp. 1828-1847.
- Kubo, M., Mizui, S. and Inonue, K. (2000) Safety Evaluation of Ship Entering a Harbor Under Severe Wave Conditions, *Proceedings of the International Offshore and Polar Engineering Conference*, 4, pp. 330-336.
- Leathrum, J., Mielke R., Mazumdar, S., Mathew, R., Manepalli, Y., Pillai, V., Malladi, R., and Jones, J. (2004) A Simulation Architecture to Support Intratheater Sealift Operations, *Mathematical and Computer Modeling*, 39, pp. 817-838.
- Ledford, G., Schneider, G. and Mock, D. (1995) Cruise Passenger Loading Bridges at Florida Ports, *Ports – Proceedings*, 1, pp. 173-184.
- Lissauer, I. And Gaines, R. (1989) Ports and Waterways Management Information System, *Coastal Zone: Proceedings of the Symposium on Coastal and Ocean Management*, 5, pp. 4065-4074.
- Luo, M. and Grigalunas, T.A. (2003) A Spatial-Economic Multimodal Transportation Simulation Model for US Coastal Container Ports, *Maritime Economics and Logistics*, 5, pp. 158-178.
- Makrinos, S. T. (2004) United States Port Security in the War Terrorism, *Sea Technology*, 45, pp. 33-34.
- Maritime and Port Security Summit (2004) *Roundtable discussion at the Maritime & Port Security Summit*, Washington, D.C.: George Washington University.
- McBride, M. (1998) Safety Assessment for Ships Manoeuvring in Ports, *Dock and Harbour Authority*, 79, pp. 142-143.
- McDonald, L. and O'Sullivan, R. (2004) Integrated Harbor Security System Enhances Port Protection, *Sea Technology*, 45, pp. 27-30.
- McGee, S. and Vann, R. (1984) Determining Channel Design Requirements for Norfolk Harbour and Channels Deepening Project, *Dock and Harbour Authority*, 65, pp. 54-56.

- Meine, J. (1998a) Automated Vessel Traffic Management, *Dock and Harbour Authority*, 78, pp. 247-248.
- Meine, J. (1998b) VTS and the Role of Information Technology, *Dock and Harbour Authority*, 79, p. 83.
- Mizui, S., Kubo, M., Sasa, K. and Nagase, S. (2003) Wave Forecast at Harbor Entrance to Support Entering Ships Under Rough Weather, *Proceedings of the International Offshore and Polar Engineering Conference*, 13, pp. 2050-2057.
- Nagle, K. (2005) Nation's Ports Concerned About Security, Harbor Dredging Funding Shortfalls in Fy'06 Budget, *The Propeller Club Quarterly*, Spring, pp. 13-14.
- Price, W. (2004) Reducing the Risk of Terror Events at Seaports, *Review of Policy Research*, 21, pp. 329-349.
- Pruitt, T. (2004) Maritime Homeland Security for Ports and Commercial Operations, *Sea Technology*, 45, pp. 20-24.
- Ronza, A., Felez, S., Darbra, R. M., Carol, S., Vilchez, J. A. and Casal, J. (2003) Predicting the Frequency of Accidents in Port Areas by Developing Event Trees from Historical Analysis, *Journal of Loss Prevention in the Process Industries*, 16, pp. 551-560.
- Savenije, R. (1997) Admittance Policy Deep Draught Vessels and Safety, *Proceedings of the International Offshore and Polar Engineering Conference*, 4, pp. 289-296.
- Savenije, R. (1998) Safety Criteria for Approach Channels, *Proceedings of the International Offshore and Polar Engineering Conference*, 4, pp. 484-491.
- Shelley, J. (2003) Terrorism on the High Seas: A Stark Reality, *Marine Log*, 108, p. 34.
- Sriskandarajah, T. and Wilkins, R. (2002) Assessment of Anchor Dragging on Gas Pipelines, *Proceedings of the International Offshore and Polar Engineering Conference*, 12, pp. 24-31.
- Staff (2003) *OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response: Guidance for Industry (Including Management and Labour), Public Authorities, Communities, and Other Stakeholders*, Paris: OECD Environment, Health and Safety Publications.
- Staff (2004a) Buoy Transmitters to Extend U.S. Port Security, *Journal of Commerce*, December 30, p. 1.
- Staff (2004b) Ports: Does Compliant Mean Secure? *Marine Log*, 109, pp. 12-14.
- Townley, J. (1989) Vessel Navigation Simulation in Ports and Harbors Development – An Update, *Coastal Zone: Proceedings of the Symposium on Coastal and Ocean Management*, 5, pp. 4481-4489.
- Trbojevic, V. M. (1998) The Use of Risk Assessment to Improve Safety Management Systems in Ports, *Dock and Harbour Authority*, 79, pp. 137-141.
- Trunick, P. A. (2004) Keeping the Ports Safe, *Logistics Today*, 45, pp. 1-2.
- U.S. Maritime Administration (2002) *Report of the United States Mobile Training Team: Regional Course on Port Security for Caribbean Countries*, Washington, D. C.: U.S. Government Printing Office.
- Ueda, S., Hirano, T., Shiraishi, S. and Yamamoto, S. (2002) Statistical Design of Fender for Berthing Ship, *Proceedings of the International Offshore and Polar Engineering Conference*, 12, pp. 545-551.
- Ueda, S., Umemura, R., Shiraishi, S., Yamamoto, S., Akakura, Y. and Yamase, S. (2001) Statistical Design of Fenders for Berthing Ship, *Proceedings of the International Offshore and Polar Engineering Conference*, 4, pp. 583-588.

- Venkatesh, V. and Wanagas, J. (1995). Integrated Port and Vessel Traffic Management Systems, *Ports–Proceedings*, 1, pp. 303-310.
- Yip, T. L., Zhang, D. H. and Chwang, A. T. (2002) Environmental and Safety Considerations for Design of a Perforated Seawall, *Proceedings of the International Offshore and Polar Engineering Conference*, 2, pp. 758-763.
- Young, W. (1995) High-Technology in Port and Vessel Operations, *Ports – Proceedings*, 1, pp. 311-322.

Appendix

Causes of Port Accidents and their Mitigation: Examples

1. Rough weather waves at a port's harbor entrance affect a ship's maneuvering (Mizui et al, 2003 and Kubo et al 2000). Perforated seawalls can be used to calm down turbulent waves in port harbors (Yip et al, 2002). Harbor tranquility analysis can be performed for developing a counter-plan for reducing the average height of a wave (Kim, 1998).
2. Berths that are inadequate for sustaining ships' berthing energy (Ueda et al, 2002 and Ueda et al, 2001). Fendering devices (e.g., rubber fenders) may be installed at berths to absorb the berthing energy of a ship and to reduce its berthing impact on the berth.
3. Pipelines in harbor waters that are susceptible to damage from ships dragging their anchor (Sriskandarajah and Wilkins, 2002).
4. Ship collisions. Approaches for reducing the risks of ship collisions in port include: a) intelligent radio data networks that relay the GPS positions of ships to a central display (Eastaugh, 1999); b) Vessel Traffic Service (VTS) systems that are integrated information networks, enabling port authorities to exercise supervision of ships and their cargoes (Meine, 1998a, 1998b; Venkatesh and Wanagas, 1995); c) real-time navigation simulation to enable port designers and engineers to evaluate proposed changes in ship navigation channels and maneuvering areas in ports (McBride, 1998; Townley, 1989; McGee and Vann, 1984); d) an admittance policy for deep-draught vessels in a port (Savenije, 1997); e) advanced navigation and information technologies to improve the operations safety of ports in conjunction with measures to improve human performance, piloting practices, pilotage administration and waterways management (Young, 1995); f) an automated information system to provide rapid access to information required for emergency response and aids to navigation management (Lissauer and Gaines, 1989); and g) a risk analysis for ship-bridge collisions (Knott et al, 1985).

5. Movement of hazardous materials. A formal safety assessment may be used to evaluate the risks in the movement of hazardous materials (Trbojevic, 1998). A policy should be developed for advising the loading, packing and labeling of hazardous cargo (Ghys, 1988). General guidance rules for preventing the spillage of hazardous materials should be developed (Staff, 2003).
6. Tidal-bound ships. A probabilistic admittance policy for tidal-bound vessels may be used to estimate the probability of a ship touching the channel bottom (Savenije, 1998).
7. Weather events. Weather continues to have a major effect on the safety of ships in ports. Improvements in weather forecasting can have significant effects on reducing weather-related port accidents (Dutton, 1998).
8. Structural failure in the anchorage system of ships. Such a failure can result in major damage to the ship if it makes contact with a fixed structure or another vessel in port before it is brought under control. Most failures occur at either the connection of the anchor chain to an anchor pile or with the failure of the pile itself (Clovis, 1998).
9. A ship breaks away from its mooring. A computer mooring analysis of a ship moored alongside a pier can be used to demonstrate how the characteristics, qualities and arrangements of mooring lines can affect the ship's mooring-line tensions experienced at the pier (Flory et al, 1998).
10. Unsafe passenger ship loading bridges. Design parameters for selecting a loading bridge for a specific ship include ship portal heights and longitudinal positions, tide and ship load line variation, ship movements and ramp slopes (Ledford et al, 1995).
11. Drug and alcohol abuse by port workers. This abuse can be addressed with drug and alcohol testing programs at ports (Harrington, 1994).